

# AUDIT REPORT

Hostname: Core  
Config file name: Core\_startup-config.cfg  
Config hash: 8b69869b6e0828a5ef9daafe4b3ff52fd948118f  
Vendor: cisco  
OS: ios  
Facility layer: core  
L3 protocols: ipv4,ipv6  
Enabled functions: ospf ipv4,eigrp named,bgp  
Date: 18/05/2020\_09:43

## SUCCESS STATISTICS

Weighted score coefficient: 55 out of 100

Successful checks: 36.5%

Unsuccessful checks: 63.5%

Total number of relevant started checks: 148

Successful checks: 54

Unsuccessful 'Critical': 23

Unsuccessful 'High': 38

Unsuccessful 'Medium': 28

Unsuccessful 'Low': 5

Unsuccessful 'Notice': 0

## Authentication, Authorization, Accounting

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	AAA new model/ Enabled AAA	High	False	False	Error <span>✗</span>
<b>Generated fix:</b> aaa new-model					
2	AAA server set	High	False	False	Error <span>✗</span>
<b>Generated fix:</b> radius server RADIUS_SERVER address ipv4 192.168.60.11 key RadKey1					
3	AAA server group	High	False	False	Error <span>✗</span>
<b>Generated fix:</b> aaa group server radius RADIUS_SERVER server name RADIUS_SERVER					
4	AAA authentication login	High	False	False	Error <span>✗</span>
<b>Generated fix:</b> aaa authentication login default group RADIUS_SERVER local enable					
5	AAA authentication login fallback	High	False	False	Error <span>✗</span>


**Generated fix:**

aaa authentication login default group RADIUS\_SERVER local enable

6	AAA authentication login only local disabled	High	False	False	Successful 
7	AAA authentication login none disabled	Critical	False	False	Successful 
8	AAA authentication "enable"	Medium	False	False	Error 

**Generated fix:**

aaa authentication enable default group RADIUS\_SERVER enable

9	AAA authentication "enable" fallback	Medium	False	False	Error 
---	--------------------------------------	--------	-------	-------	---


**Generated fix:**

aaa authentication enable default group RADIUS\_SERVER enable

10	AAA authentication "enable" only local disabled	Medium	False	False	Successful 
11	AAA authentication "enable" none disabled	High	False	False	Successful 
12	AAA authorization "exec"	High	False	False	Error 

**Generated fix:**

aaa authorization exec default group RADIUS\_SERVER local if-authenticated

13	AAA authorization "exec" fallback	High	False	False	Error 
----	-----------------------------------	------	-------	-------	---



**Generated fix:**

aaa authorization exec default group RADIUS\_SERVER local if-authenticated

14	AAA authorization "exec" only local disabled	High	False	False	Successful 
15	AAA authorization "exec" none disabled	Critical	False	False	Successful 
16	AAA accounting "connection"	High	False	False	Error 



**Generated fix:**

aaa accounting connection default start-stop group RADIUS\_SERVER

17	AAA auccounting "connection" none disabled	High	False	False	Successful 
18	AAA accounting "exec"	High	False	False	Error 

**Generated fix:**

aaa accounting exec default start-stop group RADIUS\_SERVER


19	AAA accounting "exec" none disabled	High	False	False	Successful 
20	AAA source interface	Medium	False	False	Error 

**Generated fix:**

ip radius source-interface Loopback0

21	AAA authentication max attempts less or equal to 5	High	False	False	Successful 
----	--	------	-------	-------	--

**Access to device**

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Exec timeout <=5 minutes	Medium	False	False	Error 

**Found error in context(s):**line con 0  
line vty 0 4

**Generated fix:**

line con 0  
exec-timeout 5

line vty 0 4  
exec-timeout 5

2	AUX connection input disabled	High	False	False	Successful ✓
3	AUX no execution set	High	False	False	Error ✗

**Found error in context(s):**

line aux 0

**Generated fix:**

line aux 0  
no exec

4	Remote output connections disabled	Medium	False	False	Error ✗
---	------------------------------------	--------	-------	-------	---------

**Found error in context(s):**

line con 0  
line aux 0  
line vty 0 4

**Generated fix:**

line con 0  
transport output none

line aux 0  
transport output none

line vty 0 4  
transport output none

5	Local user database with encrypted password	Critical	False	False	Error ✗
---	---	----------	-------	-------	---------

**Generated fix:**

username admin secret admin\_password

6	Local user database with plaintext password disabled	Critical	False	False	Successful ✓
7	Enable password encrypted	Critical	False	False	Error ✗

**Generated fix:**

enable secret enablepasswd123

8	Enable password plaintext disabled	Critical	False	False	Successful ✓
9	Local login to virtual terminal disabled	Critical	False	False	Error ✗

**Error configuration setting found in:**

line vty 0 4  
login

**Found error in context(s):**

line vty 0 4

10	Restrict login to device - IPv4 ACL	Critical	False	False	Error ✗
----	-------------------------------------	----------	-------	-------	---------

**Found error in context(s):**

line vty 0 4

**Generated fix:**

line vty 0 4  
access-class IPV4\_VTY\_ACL in

11	ACL specified for VTY access is created	Critical	False	False	Error ✗
----	---	----------	-------	-------	---------

**Comment:**

Cannot be fixed automatically!

**Fix notice:**

Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for managing devices with these commands:

```
ip access-list standard <acl name>
remark Permiting managemnt device
permit <ip address> <wildcard mask>
```

12	Log login to device on failure	High	False	False	Error ❌
----	--------------------------------	------	-------	-------	---------

**Generated fix:**

```
login on-failure trap
login on-failure log
login on-failure log-input
```

**Fix notice:**

Depending on IOS, usually just one of fixing command is applicable to device. There are more because of different syntax and support among IOS versions.

13	Log login to device on success	Medium	False	False	Error ❌
----	--------------------------------	--------	-------	-------	---------

**Generated fix:**

```
login on-success trap
login on-success log
login on-success log-input
```

**Fix notice:**

Depending on IOS, usually just one of fixing command is applicable to device. There are more because of different syntax and support among IOS versions.

14	Login quiet mode	Medium	False	False	Error ❌
----	------------------	--------	-------	-------	---------

**Generated fix:**

```
login quiet-mode access-class IPV4_VTY_ACL
```

15	ACL exists for specified login quiet mode	Medium	False	False	Error ❌
----	---	--------	-------	-------	---------

**Comment:**

Cannot be fixed automatically!

**Fix notice:**

Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for managing devices with these commands:

```
ip access-list standard <acl name>
remark Permiting managemnt device
permit <ip address> <wildcard mask>
```

16	One user change config at time	High	False	False	Error ❌
----	--------------------------------	------	-------	-------	---------

**Generated fix:**

```
configuration mode exclusive
configuration mode exclusive auto
```

**Fix notice:**

Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

17	Legal banner MOTD	Low	False	False	Error ❌
----	-------------------	-----	-------	-------	---------

**Generated fix:**

```
banner motd ; Unauthorized access will be prosecuted!! ;
```

18	Legal banner exec	Low	False	False	Error ❌
----	-------------------	-----	-------	-------	---------

**Generated fix:**

```
banner exec ; Unauthorized access will be prosecuted!! ;
```

19	Legal banner login	Low	False	False	Error ❌
----	--------------------	-----	-------	-------	---------

**Generated fix:**

```
banner login ; Unauthorized access will be prosecuted!! ;
```

20	Session timeout	Medium	False	False	Error ❌
----	-----------------	--------	-------	-------	---------

**Found error in context(s):**

line con 0  
line aux 0  
line vty 0 4

**Generated fix:**

line con 0  
session-timeout 30

line aux 0  
session-timeout 30

line vty 0 4  
session-timeout 30

21	AUX exec timeout one second	High	False	False	Error
----	-----------------------------	------	-------	-------	-------

**Found error in context(s):**

line aux 0

**Generated fix:**

line aux 0  
exec-timeout 0 1

22	Restrict login to device - IPv6 ACL	Critical	False	False	Error
----	-------------------------------------	----------	-------	-------	-------

**Found error in context(s):**

line vty 0 4

**Generated fix:**

line vty 0 4  
ipv6 access-class IPV6\_VTY\_ACL in

23	ACL IPv6 specified for VTY access is created	Critical	False	False	Error
----	--	----------	-------	-------	-------

**Comment:**

Cannot be fixed automatically!

**Fix notice:**

Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for managing devices with these commands:

ipv6 access-list <acl name>  
remark Permiting managemnt device  
permit ip <ip address> <wildcard mask> any

24	Login DOS block for	High	False	False	Error
----	---------------------	------	-------	-------	-------

**Generated fix:**

login block-for 120 attempts 3 within 30

## SSH

**No. Name****Severity Skipped****Cannot determine Status search/fix**

1	SSH enable on management connection	Critical	False	False	Error
---	-------------------------------------	----------	-------	-------	-------

**Found error in context(s):**

line vty 0 4

**Generated fix:**

line vty 0 4  
transport input ssh

**Fix notice:**

Make sure RSA key is present - generated or imported. For generating RSA key, issue command:  
crypto key generate rsa modulus 2048

2	SSH version 2	Critical	False	False	Error ❌
---	---------------	----------	-------	-------	---------

**Generated fix:**

ip ssh version 2

3	SSH timeout	Medium	False	False	Error ❌
---	-------------	--------	-------	-------	---------

**Generated fix:**

ip ssh timeout 30

ip ssh time-out 30

**Fix notice:**

Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

4	SSH max 3 retries	Medium	False	False	Successful ✔️
---	-------------------	--------	-------	-------	---------------

5	SSH source interface	High	False	False	Error ❌
---	----------------------	------	-------	-------	---------

**Generated fix:**

ip ssh source-interface Loopback0

6	SSH not default port	High	False	False	Error ❌
---	----------------------	------	-------	-------	---------

**Generated fix:**

ip ssh port 2223 rotary 1

7	SSH not default port applied	High	False	False	Error ❌
---	------------------------------	------	-------	-------	---------

**Found error in context(s):**

line vty 0 4

**Generated fix:**

line vty 0 4

rotary 1

## Device identification

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Hostname set	Low	False	False	Successful ✔️
<b>Comment:</b> Cannot be fixed automatically!					
<b>Right configuration setting found in:</b> hostname Core					
2	Domain name set	Low	False	False	Successful ✔️
<b>Right configuration setting found in:</b> ip domain name thesis-test.cz					
3	All interfaces have description	Low	False	False	Error ❌
<b>Comment:</b> Cannot be fixed automatically!					
<b>Right configuration setting found in:</b> interface Ethernet0/0 description WAN_PORT					

**Found port(s) with error:**

Loopback0  
Ethernet0/1  
Ethernet0/2  
Ethernet0/3  
Ethernet1/0  
Ethernet1/1  
Ethernet1/2  
Ethernet1/3  
Serial2/0  
Serial2/1  
Serial2/2  
Serial2/3  
Serial3/0  
Serial3/1  
Serial3/2  
Serial3/3

**Fix notice:**

Set interface description with command:  
interface <interface name>  
description <description of interface>

**Fix ignore comment:**

Fixing commands suppressed due to manual need of manual change and name determination.

## SNMP

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	SNMP v2 write disabled	Critical	False	False	Successful ✓
2	SNMP v2 read without ACL disabled	Critical	False	False	Successful ✓
3	SNMP v2 read with ACL disabled	Critical	False	False	Successful ✓
4	SNMP v1 trap host disabled	Critical	False	False	Successful ✓
5	SNMP v2 trap host disabled	Critical	False	False	Successful ✓
6	SNMP v3 read [authnopriv noauth authpriv without ACL] or write disabled	Critical	False	False	Successful ✓
7	SNMP v3 read authpriv with ACL enabled	Critical	False	False	Error ✗
<b>Generated fix:</b> snmp-server group SNMP_V3_GRP v3 priv read READVIEWv3 access SNMP_V3 snmp-server user SNMPv3USER SNMP_V3_GRP v3 auth sha SnmpPasswd123 priv aes 256 SnmpPasswd123 access SNMP_V3					
8	SNMP v3 read authpriv with IPv6 ACL enabled	Critical	False	False	Error ✗
<b>Generated fix:</b> snmp-server group SNMP_V3_GRP_IPV6 v3 priv read READVIEWv3 access ipv6 SNMP_V3_ACL6 snmp-server user SNMPv3USER SNMP_V3_GRP_IPV6 v3 auth sha SnmpPasswd123 priv aes 256 SnmpPasswd123 access SNMP_V3_ACL6					
9	SNMP user v1 v2c or v3 [noauth authnopriv no sha no aes without ACL] disabled	Critical	False	False	Successful ✓
10	SNMP trap source interface	High	False	False	Error ✗
<b>Generated fix:</b> snmp-server trap-source Loopback0					
11	SNMP server location	High	False	False	Error ✗
<b>Generated fix:</b> snmp-server location GNS3LAB					
12	SNMP v3 traps priv	Medium	False	False	Error ✗

**Generated fix:**

snmp-server host 192.168.60.11 version 3 priv SNMPv3USER

13	SNMP traps v3 read [authnopriv noauth] or v1 v2 disabled	Critical	False	False	Successful ✓
14	SNMP traps enabled	Medium	False	False	Error ✗

**Generated fix:**

snmp-server enable traps

15	ACL is created for SNMPv3	Critical	False	False	Error ✗
----	---------------------------	----------	-------	-------	---------

**Comment:**

Cannot be fixed automatically!

**Fix notice:**

Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for receiving SNMP with these commands:

ip access-list standard <acl name>

remark Permitting SNMP

permit <ip address> <wildcard mask>

16	ACL IPv6 is created for SNMPv3	Critical	False	False	Error ✗
----	--------------------------------	----------	-------	-------	---------

**Comment:**

Cannot be fixed automatically!

**Fix notice:**

Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for receiving SNMP with these commands:

ipv6 access-list <acl name>

remark Permitting managemnt device

permit ip <ip address> <wildcard mask> any

17	SNMP interface index persist enabled globally	High	False	False	Error ✗
----	---	------	-------	-------	---------

**Generated fix:**

snmp-server ifindex persist

snmp ifmib ifindex persist

**Fix notice:**

Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

18	SNMP interface index persist enabled per interface	High	False	False	Error ✗
----	--	------	-------	-------	---------

**Found port(s) with error:**

Loopback0

Ethernet0/0

Ethernet0/1

Ethernet0/2

Ethernet0/3

Ethernet1/0

Ethernet1/1

Ethernet1/2

Ethernet1/3

Serial2/0

Serial2/1

Serial2/2

Serial2/3

Serial3/0

Serial3/1

Serial3/2

Serial3/3



**Generated fix:**

```
interface Loopback0
snmp ifindex persist
exit
interface Ethernet0/0
snmp ifindex persist
exit
interface Ethernet0/1
snmp ifindex persist
exit
interface Ethernet0/2
snmp ifindex persist
exit
interface Ethernet0/3
snmp ifindex persist
exit
interface Ethernet1/0
snmp ifindex persist
exit
interface Ethernet1/1
snmp ifindex persist
exit
interface Ethernet1/2
snmp ifindex persist
exit
interface Ethernet1/3
snmp ifindex persist
exit
interface Serial2/0
snmp ifindex persist
exit
interface Serial2/1
snmp ifindex persist
exit
interface Serial2/2
snmp ifindex persist
exit
interface Serial2/3
snmp ifindex persist
exit
interface Serial3/0
snmp ifindex persist
exit
interface Serial3/1
snmp ifindex persist
exit
interface Serial3/2
snmp ifindex persist
exit
interface Serial3/3
snmp ifindex persist
exit
```

## Syslog

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Syslog server enabled	High	False	False	Error ❌
<b>Generated fix:</b> logging host 192.168.60.11					
2	Syslog server IPv6 enabled	High	False	False	Error ❌
<b>Generated fix:</b> logging host ipv6 fd00:60::2050:79ff:fe66:6805					
3	Syslog source interface	Medium	False	False	Error ❌
<b>Generated fix:</b> logging source-interface Loopback0					
4	Syslog format	Medium	False	False	Successful ✅

**Right configuration setting found in:**

service timestamps log datetime msec

5	Syslog critical alerts to console	Medium	False	False	Error ❌
---	-----------------------------------	--------	-------	-------	---------

**Generated fix:**

logging console critical

6	Syslog send informational traps	High	False	False	Successful ✔
---	---------------------------------	------	-------	-------	--------------

7	Syslog buffer set with severity	High	False	False	Error ❌
---	---------------------------------	------	-------	-------	---------

**Generated fix:**

logging buffered 40960 informational

8	Syslog local backup	High	False	False	Error ❌
---	---------------------	------	-------	-------	---------

**Generated fix:**

logging persistent url flash:

9	Syslog sequence numbers added	Medium	False	False	Error ❌
---	-------------------------------	--------	-------	-------	---------

**Generated fix:**

service sequence-numbers

## NTP

No.	Name	Severity	Skipped	Cannot determine Status search/fix
1	NTP server set	High	False	False Error ❌

**Generated fix:**

ntp server 192.168.60.11

2	NTP source interface	Medium	False	False Error ❌
---	----------------------	--------	-------	---------------

**Generated fix:**

ntp source Loopback0

3	NTP authentication key	High	False	False Error ❌
---	------------------------	------	-------	---------------

**Generated fix:**

ntp authentication-key 1 md5 ntpPasswd123

4	NTP trusted key	High	False	False Error ❌
---	-----------------	------	-------	---------------

**Generated fix:**

ntp trusted-key 1

5	NTP authenticate	High	False	False Error ❌
---	------------------	------	-------	---------------

**Generated fix:**

ntp authenticate

## High load

No.	Name	Severity	Skipped	Cannot determine Status search/fix
1	SNMP traps for CPU load	Medium	False	False Error ❌

**Generated fix:**

snmp-server enable traps cpu threshold

2	Threshold for CPU load	Medium	False	False Error ❌
---	------------------------	--------	-------	---------------

**Generated fix:**

process cpu threshold type total rising 70 interval 5

3	Statistics entry for CPU load	Low	False	False	Error ❌
---	-------------------------------	-----	-------	-------	---------

**Generated fix:**

process cpu statistics limit entry-percentage 70

4	Reserve memory for critical notification	Medium	False	False	Error ❌
---	--	--------	-------	-------	---------

**Generated fix:**

memory reserve critical 1000

5	Minimum CPU memory notification	Medium	False	False	Error ❌
---	---------------------------------	--------	-------	-------	---------

**Generated fix:**

memory free low-watermark processor 2000

6	Minimum IO memory notification	Medium	False	False	Error ❌
---	--------------------------------	--------	-------	-------	---------

**Generated fix:**

memory free low-watermark io 2000

## Network Mapping

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	CDP globally disabled	Critical	False	False	Error ❌

**Generated fix:**

no cdp run

**Fix notice:**

Services such as Cisco IP telephony would not work

2	CDP disabled on interface(s)	Critical	False	False	Error ❌
---	------------------------------	----------	-------	-------	---------

**Found port(s) with error:**

Ethernet0/0  
Ethernet0/1  
Ethernet0/2  
Ethernet0/3  
Ethernet1/0  
Ethernet1/1  
Ethernet1/2  
Ethernet1/3  
Serial2/0  
Serial2/1  
Serial2/2  
Serial2/3  
Serial3/0  
Serial3/1  
Serial3/2  
Serial3/3

**Generated fix:**

```
interface Ethernet0/0
no cdp enable
exit
interface Ethernet0/1
no cdp enable
exit
interface Ethernet0/2
no cdp enable
exit
interface Ethernet0/3
no cdp enable
exit
interface Ethernet1/0
no cdp enable
exit
interface Ethernet1/1
no cdp enable
exit
interface Ethernet1/2
no cdp enable
exit
interface Ethernet1/3
no cdp enable
exit
interface Serial2/0
no cdp enable
exit
interface Serial2/1
no cdp enable
exit
interface Serial2/2
no cdp enable
exit
interface Serial2/3
no cdp enable
exit
interface Serial3/0
no cdp enable
exit
interface Serial3/1
no cdp enable
exit
interface Serial3/2
no cdp enable
exit
interface Serial3/3
no cdp enable
exit
```

3	LLDP globally disabled	Critical	False	False	Successful ✓
4	LLDP receive disabled on interface(s)	Critical	False	False	Not relevant ✓

**Comment:**  
Module 11\_04\_lldp\_receive.yaml configured to run after 11\_03\_lldp\_run\_disabled.yaml with status error but that module has not run yet with specified cmd\_match\_status, 11\_04\_lldp\_receive.yaml will not run

5	LLDP transmit disabled on interface(s)	Critical	False	False	Not relevant ✓
---	--	----------	-------	-------	----------------

**Comment:**  
Module 11\_05\_lldp\_transmit.yaml configured to run after 11\_03\_lldp\_run\_disabled.yaml with status error but that module has not run yet with specified cmd\_match\_status, 11\_05\_lldp\_transmit.yaml will not run

6	Proxy ARP disabled on interface(s)	Critical	False	False	Error ✗
---	------------------------------------	----------	-------	-------	---------

**Found port(s) with error:**

Loopback0  
Ethernet0/0  
Ethernet0/1  
Ethernet0/2  
Ethernet0/3  
Ethernet1/0  
Ethernet1/1  
Ethernet1/2  
Ethernet1/3  
Serial2/0  
Serial2/1  
Serial2/2  
Serial2/3  
Serial3/0  
Serial3/1  
Serial3/2  
Serial3/3

**Generated fix:**

```
interface Loopback0
no ip proxy-arp
exit
interface Ethernet0/0
no ip proxy-arp
exit
interface Ethernet0/1
no ip proxy-arp
exit
interface Ethernet0/2
no ip proxy-arp
exit
interface Ethernet0/3
no ip proxy-arp
exit
interface Ethernet1/0
no ip proxy-arp
exit
interface Ethernet1/1
no ip proxy-arp
exit
interface Ethernet1/2
no ip proxy-arp
exit
interface Ethernet1/3
no ip proxy-arp
exit
interface Serial2/0
no ip proxy-arp
exit
interface Serial2/1
no ip proxy-arp
exit
interface Serial2/2
no ip proxy-arp
exit
interface Serial2/3
no ip proxy-arp
exit
interface Serial3/0
no ip proxy-arp
exit
interface Serial3/1
no ip proxy-arp
exit
interface Serial3/2
no ip proxy-arp
exit
interface Serial3/3
no ip proxy-arp
exit
```

7	ICMP Unreachable disabled on interface(s)	High	False	False	Error <span style="color: red;">✗</span>
---	---	------	-------	-------	--


**Found port(s) with error:**

Loopback0  
 Ethernet0/0  
 Ethernet0/1  
 Ethernet0/2  
 Ethernet0/3  
 Ethernet1/0  
 Ethernet1/1  
 Ethernet1/2  
 Ethernet1/3  
 Serial2/0  
 Serial2/1  
 Serial2/2  
 Serial2/3  
 Serial3/0  
 Serial3/1  
 Serial3/2  
 Serial3/3

**Generated fix:**

```

interface Loopback0
no ip unreachable
exit
interface Ethernet0/0
no ip unreachable
exit
interface Ethernet0/1
no ip unreachable
exit
interface Ethernet0/2
no ip unreachable
exit
interface Ethernet0/3
no ip unreachable
exit
interface Ethernet1/0
no ip unreachable
exit
interface Ethernet1/1
no ip unreachable
exit
interface Ethernet1/2
no ip unreachable
exit
interface Ethernet1/3
no ip unreachable
exit
interface Serial2/0
no ip unreachable
exit
interface Serial2/1
no ip unreachable
exit
interface Serial2/2
no ip unreachable
exit
interface Serial2/3
no ip unreachable
exit
interface Serial3/0
no ip unreachable
exit
interface Serial3/1
no ip unreachable
exit
interface Serial3/2
no ip unreachable
exit
interface Serial3/3
no ip unreachable
exit
  
```

8	ICMPv6 Unreachable disabled on interface(s)	High	False	False	Error 
---	---	------	-------	-------	---

**Found port(s) with error:**

Loopback0  
Ethernet0/0  
Ethernet0/1  
Ethernet0/2  
Ethernet0/3  
Ethernet1/0  
Ethernet1/1  
Ethernet1/2  
Ethernet1/3  
Serial2/0  
Serial2/1  
Serial2/2  
Serial2/3  
Serial3/0  
Serial3/1  
Serial3/2  
Serial3/3

**Generated fix:**

```
interface Loopback0
no ipv6 unreachable
exit
interface Ethernet0/0
no ipv6 unreachable
exit
interface Ethernet0/1
no ipv6 unreachable
exit
interface Ethernet0/2
no ipv6 unreachable
exit
interface Ethernet0/3
no ipv6 unreachable
exit
interface Ethernet1/0
no ipv6 unreachable
exit
interface Ethernet1/1
no ipv6 unreachable
exit
interface Ethernet1/2
no ipv6 unreachable
exit
interface Ethernet1/3
no ipv6 unreachable
exit
interface Serial2/0
no ipv6 unreachable
exit
interface Serial2/1
no ipv6 unreachable
exit
interface Serial2/2
no ipv6 unreachable
exit
interface Serial2/3
no ipv6 unreachable
exit
interface Serial3/0
no ipv6 unreachable
exit
interface Serial3/1
no ipv6 unreachable
exit
interface Serial3/2
no ipv6 unreachable
exit
interface Serial3/3
no ipv6 unreachable
exit
```

9	ICMP Mask Reply disabled on interface(s)	High	False	False	Successful ✓
10	Directed broadcast disabled on interface(s)	Critical	False	False	Successful ✓
11	ICMP Redirects disabled on interface(s)	High	False	False	Error ✗

**Found port(s) with error:**

```
Loopback0
Ethernet0/0
Ethernet0/1
Ethernet0/2
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Serial2/0
Serial2/1
Serial2/2
Serial2/3
Serial3/0
Serial3/1
Serial3/2
Serial3/3
```



**Generated fix:**

```
interface Loopback0
no ip redirects
exit
interface Ethernet0/0
no ip redirects
exit
interface Ethernet0/1
no ip redirects
exit
interface Ethernet0/2
no ip redirects
exit
interface Ethernet0/3
no ip redirects
exit
interface Ethernet1/0
no ip redirects
exit
interface Ethernet1/1
no ip redirects
exit
interface Ethernet1/2
no ip redirects
exit
interface Ethernet1/3
no ip redirects
exit
interface Serial2/0
no ip redirects
exit
interface Serial2/1
no ip redirects
exit
interface Serial2/2
no ip redirects
exit
interface Serial2/3
no ip redirects
exit
interface Serial3/0
no ip redirects
exit
interface Serial3/1
no ip redirects
exit
interface Serial3/2
no ip redirects
exit
interface Serial3/3
no ip redirects
exit
```

## Routing

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	OSPF IPv4 Router ID	Medium	False	False	Successful ✓
<b>Right configuration setting found in:</b> router ospf 1 router-id 10.10.10.1					
2	OSPF IPv6 Router ID	Medium	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function ospf ipv6 not configured on device. Everything is OK.					
3	OSPFv3 Address Family General Router ID	Medium	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function ospfv3 not configured on device. Everything is OK.					
4	OSPFv3 Address Family IPv4 Router ID	Medium	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function ospfv3 not configured on device. Everything is OK.					
5	OSPFv3 Address Family IPv6 Router ID	Medium	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function ospfv3 not configured on device. Everything is OK.					
6	EIGRP IPv4 Router ID	Medium	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function eigrp ipv4 not configured on device. Everything is OK.					
7	EIGRP IPv6 Router ID	Medium	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function eigrp ipv6 not configured on device. Everything is OK.					
8	EIGRP Named IPv4 Router ID	Medium	False	False	Successful ✓
<b>Right configuration setting found in:</b> router eigrp EIGRP_NAMED address-family ipv4 unicast autonomous-system 1 eigrp router-id 10.10.10.1					
9	EIGRP Named IPv6 Router ID	Medium	False	False	Successful ✓
<b>Right configuration setting found in:</b> router eigrp EIGRP_NAMED address-family ipv6 unicast autonomous-system 1 eigrp router-id 10.10.10.1					
10	BGP Router ID	Medium	False	False	Error ✗
<b>Found error in context(s):</b> router bgp 1211  <b>Generated fix:</b> router bgp 1211 bgp router-id 3.3.3.3					
11	OSPF IPv4 Log adjacency changes	Medium	False	False	Successful ✓
12	OSPF IPv6 Log adjacency changes	Medium	True	False	Not relevant ✓

<b>Comment:</b> Skipped, required function ospf ipv6 not configured on device. Everything is OK.					
13	OSPFv3 Address Family IPv6 Log adjacency changes	Medium	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function ospfv3 not configured on device. Everything is OK.					
14	OSPFv3 Address Family IPv4 Log adjacency changes	Medium	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function ospfv3 not configured on device. Everything is OK.					
15	OSPFv3 Address Family IPv6 Log adjacency changes	Medium	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function ospfv3 not configured on device. Everything is OK.					
16	EIGRP IPv4 Log neighbor changes	Medium	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function eigrp ipv4 not configured on device. Everything is OK.					
17	EIGRP IPv6 Log neighbor changes	Medium	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function eigrp ipv6 not configured on device. Everything is OK.					
18	EIGRP Named IPv4 Log neighbor changes	Medium	False	False	Successful ✓
19	EIGRP Named IPv6 Log neighbor changes	Medium	False	False	Successful ✓
20	BGP Log neighbor changes	Medium	False	False	Successful ✓
<b>Right configuration setting found in:</b> router bgp 1211 bgp log-neighbor-changes					
21	RIP auto summary disabled	High	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function rip not configured on device. Everything is OK.					
22	EIGRP IPv4 Auto summary disabled	High	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function eigrp ipv4 not configured on device. Everything is OK.					
23	EIGRP IPv6 Auto summary disabled	High	True	False	Not relevant ✓
<b>Comment:</b> Skipped, required function eigrp ipv6 not configured on device. Everything is OK.					
24	EIGRP Named IPv4 Auto summary disabled	High	False	False	Successful ✓
25	EIGRP Named IPv6 Auto summary disabled	High	False	False	Successful ✓
26	BGP Auto summary disabled	High	False	False	Successful ✓
27	BGP Multihop disabled or TTL security used	High	False	False	Successful ✓
28	IP Source routing (IP Options) disabled	Critical	False	False	Successful ✓

## Filtering

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	ACL filter specified for IPv4 addresses on WAN	Critical	False	False	Error ✗

**Generated fix:**

```
ip access-list extended IPV4_WAN_FILTER
remark DENY RFC6890 and RFC8190
deny ip 0.0.0.0 0.255.255.255 any log-input
deny ip 10.0.0.0 0.255.255.255 any log-input
deny ip 100.64.0.0 0.63.255.255 any log-input
deny ip 127.0.0.0 0.255.255.255 any log-input
deny ip 169.254.0.0 0.0.255.255 any log-input
deny ip 172.16.0.0 0.15.255.255 any log-input
deny ip 192.0.0.0 0.0.0.7 any log-input
deny ip 192.0.2.0 0.0.0.255 any log-input
deny ip 192.18.0.0 0.1.255.255 any log-input
deny ip 198.51.100.0 0.0.0.255 any log-input
deny ip 192.168.0.0 0.0.255.255 any log-input
deny ip 192.0.0.0 0.255.255.255 any log-input
deny ip 203.0.113.0 0.0.0.255 any log-input
deny ip 224.0.0.0 15.255.255.255 any log-input
deny ip 240.0.0.0 15.255.255.255 any log-input
permit ip any any
```

**Fix notice:**

Some devices do not recognize parameter "log-input" in ACL, so manually replace it with "log"

2	ACL filter IPv4 applied on WAN interface	Critical	False	False	Error ❌
---	--	----------	-------	-------	---------

**Found port(s) with error:**

Ethernet0/0

**Generated fix:**

```
interface Ethernet0/0
ip access-group IPV4_WAN_FILTER in
exit
```

**Fix notice:**

ACL will be applied to specified WAN interface. In case of existing ACL on interface in same direction, please set variable fix\_cmd\_ignore: "true" and append generated ACL from module 13\_01\_ipv4\_filter\_wan to existing ACL to proper place.

3	ACL filter specified for IPv5 addresses on WAN	Critical	False	False	Error ❌
---	--	----------	-------	-------	---------

**Generated fix:**

```
ipv6 access-list IPV6_WAN_FILTER
remark DENY RFC6890 and RFC8190 and RFC5156
deny ipv6 host ::1 any log-input
deny ipv6 host :: any log-input
deny ipv6 ::FFFF:0.0.0.0/96 any log-input
deny ipv6 100::/64 any log-input
deny ipv6 2001::/23 any log-input
deny ipv6 2001::/32 any log-input
deny ipv6 2001:2::/48 any log-input
deny ipv6 2001:DB8::/32 any log-input
deny ipv6 2001:10::/28 any log-input
deny ipv6 2002::/16 any log-input
deny ipv6 FC00::/7 any log-input
deny ipv6 FF00::/8 any log-input
permit ipv6 any any
```

**Fix notice:**

Some devices do not recognize parameter "log-input" in ACL, so manually replace it with "log"

4	ACL filter IPv6 applied on WAN interface	Critical	False	False	Error ❌
---	--	----------	-------	-------	---------

**Found port(s) with error:**

Ethernet0/0

**Generated fix:**

```
interface Ethernet0/0
ipv6 traffic-filter IPV6_WAN_FILTER in
exit
```

**Fix notice:**

ACL will be applied to specified WAN interface. In case of existing ACL on interface in same direction, please set variable fix\_cmd\_ignore: "true" and append generated ACL from module 13\_03\_ipv6\_filter\_wan to existing ACL to proper place.


5	IP Options disabled	Critical	False	False	Error ❌
---	---------------------	----------	-------	-------	---------

**Generated fix:**

ip options drop

**Fix notice:**

RSVP and other protocols that use IP Options packets may not function as expected.

6	ACL filter IPv6 unknown extended header	Critical	False	False	Error 
---	---	----------	-------	-------	---

**Generated fix:**

```
ipv6 access-list IPV6_FRAGMENT_FILTER
remark DENY unknown IPv6 extended headers
deny ipv6 any any undetermined-transport log-input
permit ipv6 any any
```

**Fix notice:**

Some devices do not recognize parameter "log-input" in ACL, so manually replace it with "log"

7	ACL filter IPv6 unknown extended header applied on WAN interface	Critical	False	False	Error 
---	--	----------	-------	-------	---

**Found port(s) with error:**

Ethernet0/0

**Generated fix:**

```
interface Ethernet0/0
ipv6 traffic-filter IPV6_FRAGMENT_FILTER in
exit
```

**Fix notice:**

ACL will be applied to specified WAN interface. In case of existing ACL on interface in same direction, please set variable fix\_cmd\_ignore: "true" and append generated ACL from module 13\_06\_ipv6\_extended\_header.yaml to existing ACL to proper place.

## Other


No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Servis PAD disabled (Packet assembler disassembler)	High	False	False	Error 
<b>Generated fix:</b> no service pad					
2	BOOTP server disabled	High	False	False	Error 
<b>Generated fix:</b> no ip bootp server					
3	Ident protocol disabled	High	False	False	Successful 
4	Finger protocol disabled	High	False	False	Successful 
5	HTTP server disabled	High	False	False	Successful 
6	HTTPS server disabled	High	False	False	Successful 
7	TCP small server disabled	High	False	False	Successful 
8	UDP small server disabled	High	False	False	Successful 
9	MOP protocol disabled	High	False	False	Error 

**Found port(s) with error:**

Ethernet0/0  
Ethernet0/1  
Ethernet0/2  
Ethernet0/3  
Ethernet1/0  
Ethernet1/1  
Ethernet1/2  
Ethernet1/3  
Serial2/0  
Serial2/1  
Serial2/2  
Serial2/3  
Serial3/0  
Serial3/1  
Serial3/2  
Serial3/3


**Generated fix:**

interface Ethernet0/0  
no mop enabled  
exit  
interface Ethernet0/1  
no mop enabled  
exit  
interface Ethernet0/2  
no mop enabled  
exit  
interface Ethernet0/3  
no mop enabled  
exit  
interface Ethernet1/0  
no mop enabled  
exit  
interface Ethernet1/1  
no mop enabled  
exit  
interface Ethernet1/2  
no mop enabled  
exit  
interface Ethernet1/3  
no mop enabled  
exit  
interface Serial2/0  
no mop enabled  
exit  
interface Serial2/1  
no mop enabled  
exit  
interface Serial2/2  
no mop enabled  
exit  
interface Serial2/3  
no mop enabled  
exit  
interface Serial3/0  
no mop enabled  
exit  
interface Serial3/1  
no mop enabled  
exit  
interface Serial3/2  
no mop enabled  
exit  
interface Serial3/3  
no mop enabled  
exit

10	IP domain lookup disabled	High	False	False	Successful 
----	---------------------------	------	-------	-------	--


**Right configuration setting found in:**

no ip domain lookup

11	Gratuitous ARPs generation disabled	High	False	False	Error 
----	-------------------------------------	------	-------	-------	---

**Generated fix:**

no ip gratuitous-arps

12	Gratuitous ARPs reject enabled	High	False	False	Error 
----	--------------------------------	------	-------	-------	---

**Generated fix:**

ip arp gratuitous none

13	Netflow is disabled	Notice	False	False	Successful ✓
----	---------------------	--------	-------	-------	--------------

**Fix ignore comment:**

By default fix is ignored due to disablement of traffic monitoring. Consider whether port mirroring is necessary for monitoring

14	Netflow version 9 used	Medium	False	False	Not relevant ✓
----	------------------------	--------	-------	-------	----------------

**Comment:**

Module 15\_14\_netflow\_version\_9.yaml configured to run after 15\_13\_netflow.yaml with status error but that module has not run yet with specified cmd\_match\_status, 15\_14\_netflow\_version\_9.yaml will not run

15	Netflow traffic analyze disabled on interface(s)	Notice	False	False	Not relevant ✓
----	--	--------	-------	-------	----------------

**Comment:**

Module 15\_15\_netflow\_interface.yaml configured to run after 15\_13\_netflow.yaml with status error but that module has not run yet with specified cmd\_match\_status, 15\_15\_netflow\_interface.yaml will not run

**Fix ignore comment:**

By default fix is ignored due to disablement of traffic monitoring. Consider whether port mirroring is necessary for monitoring

16	Port mirroring disabled on interface(s)	Notice	False	False	Successful ✓
----	---	--------	-------	-------	--------------

**Fix ignore comment:**

By default fix is ignored due to disablement of traffic monitoring. Consider whether port mirroring is necessary for monitoring

17	Set always "UP" Loopback interface with IP address	Medium	False	False	Successful ✓
----	--	--------	-------	-------	--------------

**Right configuration setting found in:**

interface Loopback0  
ip address 10.10.10.20 255.255.255.255  
ip ospf network point-to-point

18	Notification on memory IO leak/overflow	Medium	False	False	Error ✗
----	---	--------	-------	-------	---------

**Generated fix:**

exception memory ignore overflow io

19	Notification on memory CPU leak/overflow	Medium	False	False	Error ✗
----	--	--------	-------	-------	---------

**Generated fix:**

exception memory ignore overflow processor

20	Network boot disabled	Medium	False	False	Successful ✓
----	-----------------------	--------	-------	-------	--------------

21	Network config load disabled	Medium	False	False	Successful ✓
----	------------------------------	--------	-------	-------	--------------

22	SCP server enabled	Medium	False	False	Error ✗
----	--------------------	--------	-------	-------	---------

**Generated fix:**

ip scp server enable

23	SCP alias copy instead of TFTP	High	False	False	Successful ✓
----	--------------------------------	------	-------	-------	--------------

24	Protection of configuration deletion	High	False	False	Error ✗
----	--------------------------------------	------	-------	-------	---------

**Generated fix:**

secure boot config  
secure boot-config

**Fix notice:**

Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

25	Archive and log config changes	Medium	False	False	Error ✗
----	--------------------------------	--------	-------	-------	---------

**Generated fix:**

archive  
path unix:  
log config  
logging enable  
notify syslog  
hidekeys  
maximum 5  
time-period 60

26	Terminate hanged inbound TCP connection to device	Medium	False	False	Error ❌
----	---	--------	-------	-------	---------

**Generated fix:**

service tcp-keepalives-in

27	Terminate hanged outbound TCP connection to device	Medium	False	False	Error ❌
----	--	--------	-------	-------	---------

**Generated fix:**

service tcp-keepalives-out

28	Encrypt all saved passwords in configuration	Critical	False	False	Successful ✔
----	--	----------	-------	-------	--------------

**Right configuration setting found in:**

no service password-encryption